SOLE INVENTOR

"EXPRESS MAIL" mailing label No. EL564459977US.
Date of Deposit: July 6, 2001
I hereby certify that this paper (or fee) is being deposited with the United States Postal Service "EXPRESS MAIL POST OFFICE TO ADDRESSEE" service under 37 CFR §1.10 on the date indicated above and is addressed to: Commissioner for Patents, Washington, D.C. 20231

Laura Frasher
Laura Frasher

APPLICATION FOR UNITED STATES LETTERS PATENT

S P E C I F I C A T I O N

TO ALL WHOM IT MAY CONCERN:

Be it known that I, Maurice Milgram, a citizen of France, residing at 7 place Pinel, 75013 Paris, France have invented a new and useful METHOD OF SECURIZATION UTILIZING OPTICAL TRANSMISSION OF INFORMATION, of which the following is a specification.

Procédé de sécurisation utilisant une transmission d'information par voie optique et disque optique pour la mise en œuvre de ce procédé.

La présente invention est relative aux procédés de sécurisation utilisant une transmission d'information par voie optique et aux disques optiques pour la mise en œuvre de ces procédés.

Plus particulièrement, l'invention concerne un procédé de sécurisation utilisant une transmission d'information par voie optique entre d'une part, un appareil électronique utilisateur (notamment : micro-ordinateur, terminal de paiement, distributeur de monnaie réelle ou électronique, terminal de contrôle d'accès, etc., ou tout autre appareil utilisateur d'un dispositif électronique de sécurisation) qui comprend au moins une interface d'entrée et un écran, et d'autre part, un dispositif électronique de sécurisation qui comprend :

- une interface de réception comprenant au moins un capteur optique pour recevoir des informations d'entrée provenant de l'appareil électronique utilisateur,
- une interface d'émission adaptée pour émettre des informations de sortie en fonction au moins des informations d'entrée reçues, ces informations de sortie correspondant (directement ou indirectement) à un code de sécurisation destiné à être communiqué à l'interface d'entrée de l'appareil électronique utilisateur,
- et une unité centrale électronique reliée aux interfaces de réception et d'émission et adaptée pour déterminer les informations de sortie en fonction au moins des informations d'entrée et pour faire émettre lesdites informations de sortie par l'interface d'émission,

le procédé de sécurisation comprenant les étapes suivan-

tes :

(a) faire transmettre les informations d'entrée par le dispositif électronique utilisateur à l'interface de réception du dispositif électronique de sécurisation,

(b) faire déterminer les informations de sortie par l'unité centrale du dispositif électronique de sécurisation, en fonction des informations d'entrée,

(c) faire émettre par l'interface de sortie du dispositif électronique de sécurisation, les informations de sortie correspondant au code de sécurisation, et communiquer ce code de sécurisation à l'appareil électronique utilisateur, par l'intermédiaire de l'interface d'entrée dudit appareil électronique utilisateur,

(d) et en vérifier que le code de sécurisation reçu par l'appareil électronique utilisateur est relié aux informations d'entrée par une relation prédéterminée, notamment pour autoriser ou non certaines opérations réalisées au moyen dudit appareil électronique utilisateur (les opérations en question peuvent être réalisées directement par l'appareil électronique utilisateur, ou le cas échéant par un appareil électronique distant relié audit appareil utilisateur).

Le document US-A-5 652 838 décrit un exemple de procédé utilisant un tel dispositif électronique de sécurisation, intégré en l'occurrence dans un disque optique. L'interface d'entrée est constituée par des capteurs optiques adaptés pour détecter le rayon laser de lecture d'un ordinateur utilisant le disque optique, lequel rayon laser est commandé de façon que sa séquence de passage sur les capteurs optiques corresponde à un certain code d'entrée. L'interface de sortie du disque optique est constituée par un écran qui affiche un code de sortie en fonction du code d'entrée reçu de l'ordinateur. L'utilisateur doit sortir

le disque optique de son lecteur pour lire le code de sortie, après quoi ledit utilisateur tape ce code sur le clavier de son ordinateur, ce qui autorise l'utilisation du disque optique par l'ordinateur. On se prémunit ainsi contre les copies illicites du disque optique.

Ces dispositions paraissent très séduisantes, puisqu'elles permettent de transmettre des informations vers le disque optique au moyen du faisceau de lecture déjà prévu pour lire ce disque.

Mais lesdites dispositions présentent l'inconvénient d'obliger à placer les capteurs optiques dans la zone de données du disque pour que ces capteurs puissent recevoir le faisceau de lecture, d'où des contraintes quant à la disposition des données dans ladite zone de stockage de données et des limitations de capacité de ladite zone de données.

De plus, cette solution n'est utilisable qu'avec un disque optique et non avec un dispositif électronique de sécurisation intégré dans un autre support de données ou constituant un appareil autonome indépendant d'un support de données.

La présente invention a notamment pour but de pallier ces inconvénients.

A cet effet, selon l'invention, un procédé de sécurisation du genre en question est caractérisé en ce qu'au cours de l'étape (a), on place le capteur optique du dispositif électronique de sécurisation face à l'écran de l'appareil électronique utilisateur, et on fait émettre par ledit écran un signal lumineux modulé porteur des informations d'entrée.

Lorsque le dispositif électronique de sécurisation est intégré dans un disque optique, on évite ainsi les contraintes susmentionnées relatives à la capacité de la

zone de données et à la disposition des données dans ladite zone de données, puisque dans ce cas, il n'est plus obligatoire de placer le capteur optique dans la zone de données lorsque le support de données est un disque optique.

De plus, cette solution technique est utilisable non seulement pour les supports de données à lecture optique, mais également pour d'autres types de supports de données, notamment à lecture magnétique, ainsi que pour d'autres dispositifs tels que des badges ou autres.

Dans des modes de réalisation préférés de l'invention, on peut éventuellement avoir recours en outre à l'une et/ou à l'autre des dispositions suivantes :

- au cours de l'étape (d), on autorise ou non certaines opérations réalisées au moyen de l'appareil électronique utilisateur, en fonction de la vérification du code de sécurisation ;
- le dispositif électronique de sécurisation appartient à un support portatif de données numériques lisible par l'appareil électronique utilisateur ;
- le support de données utilisé est un disque optique comprenant une zone de données annulaire entourant une partie centrale dépourvue de données numériques, laquelle partie centrale comprend le capteur optique ;
- au cours de l'étape (a), ledit signal lumineux modulé est émis dans une zone prédéterminée appartenant à l'écran, et on place le capteur optique du dispositif électronique de sécurisation au voisinage immédiat de ladite zone prédéterminée ;
- au cours de l'étape (a), ladite zone prédéterminée de l'écran est signalée par au moins un repère affiché par l'écran ;
- au cours de l'étape (c), les informations de

sortie sont émises par le dispositif électronique de sécurisation sous forme d'un signal acoustique ;

- le signal acoustique contenant les informations de sortie est écouté par un opérateur humain, lequel opérateur détermine le code de sécurisation en fonction du signal écouté (ledit code de sécurisation peut le cas échéant être constitué par les informations de sortie elles-mêmes) et communique ce code de sécurisation à l'appareil électronique utilisateur par l'intermédiaire de son interface d'entrée ;

- le signal acoustique contenant les informations de sortie est reçu directement par l'interface d'entrée de l'appareil électronique utilisateur ;

- le signal acoustique contenant les informations de sortie est transmis à un poste de contrôle distant qui détermine le code de sécurisation en fonction dudit signal acoustique et transmet ce code de sécurisation à l'interface d'entrée de l'appareil électronique utilisateur ;

- au cours de l'étape (c), les informations de sortie sont émises par le dispositif électronique de sécurisation par affichage sur un dispositif d'affichage ;

- on fait échanger des données codées entre d'une part, un poste central distant communiquant avec l'appareil électronique utilisateur, et d'autre part, l'unité centrale du support de données, par l'intermédiaire des interfaces d'émission et de réception dudit dispositif électronique de sécurisation (on peut ainsi notamment identifier l'utilisateur en fonction des données codées échangées entre le poste central distant et l'unité centrale du dispositif électronique de sécurisation, pour sécuriser une opération à distance, par exemple une opération de paiement à distance ou autre) ;

- le dispositif électronique de sécurisation a en

mémoire un compte d'unités de valeur, et l'unité centrale dudit dispositif de sécurisation est adaptée pour faire varier ledit compte d'unités de valeur en fonction de données codées reçues et émises par l'unité centrale par l'intermédiaire des interfaces de réception et d'émission ;

- le dispositif électronique de sécurisation appartient à un support de données qui est lisible par l'appareil électronique utilisateur avec mise en mouvement dudit support de données, le dispositif électronique de sécurisation ayant en mémoire au moins un compteur d'unités d'utilisation, et l'unité centrale dudit dispositif de sécurisation fait varier ledit compteur en fonction des mouvements du support de données détectés par un capteur de mouvement ;

- on fait lire le compteur d'unités d'utilisation par un lecteur externe, au moyen d'une interface de communication appartenant audit dispositif de sécurisation ;

- le procédé comprend une étape d'activation d'au moins certaines fonctions du dispositif électronique de sécurisation, étape au cours de laquelle on communique un code d'accès prédéterminé à l'unité centrale dudit dispositif électronique de sécurisation .

- au cours de l'étape d'activation, on communique le code d'accès à l'unité centrale au moyen d'une interface d'entrée du dispositif électronique de sécurisation actionnable par un utilisateur ;

- au cours de l'étape d'activation, on communique le code d'accès à l'unité centrale en positionnant successivement le capteur optique du dispositif électronique de sécurisation en correspondance avec plusieurs zones prédéterminées appartenant à l'écran de l'appareil électronique utilisateur, ces différentes zones prédéterminées de

l'écran émettant respectivement différents signaux optiques prédéterminés et correspondant chacun à un symbole affiché sur l'écran ;

- pour communiquer le code d'accès à l'unité centrale du dispositif électronique de sécurisation, on communique d'abord ce code d'accès à l'appareil électronique utilisateur en utilisant l'interface d'entrée dudit appareil électronique utilisateur, on place le capteur optique du dispositif électronique de sécurisation face à l'écran de l'appareil électronique utilisateur, et on fait émettre par ledit écran un signal lumineux modulé correspondant audit code d'accès ;

- au cours de l'étape (b), on fait déterminer les informations de sortie par l'unité centrale du dispositif électronique de sécurisation en fonction des informations d'entrée et d'un code personnel précédemment communiqué par l'utilisateur du dispositif électronique de sécurisation à ladite unité centrale ;

- au cours de l'étape (b), on communique le code personnel à l'unité centrale du dispositif électronique de sécurisation au moyen d'une interface d'entrée du dispositif électronique de sécurisation, actionnable par un utilisateur ;

- au cours de l'étape (b), on communique le code personnel à l'unité centrale électronique en positionnant successivement le capteur optique du dispositif électronique de sécurisation en correspondance avec plusieurs zones prédéterminées appartenant à l'écran de l'appareil électronique utilisateur, ces différentes zones prédéterminées de l'écran émettant respectivement différents signaux optiques prédéterminés et correspondant chacun à un symbole affiché sur l'écran ;

- au cours de l'étape (b), pour communiquer le

code personnel à l'unité centrale du dispositif électronique de sécurisation, on communique d'abord ce code personnel à l'appareil électronique utilisateur en utilisant l'interface d'entrée dudit appareil électronique utilisateur, on place le capteur optique du dispositif électronique de sécurisation face à l'écran de l'appareil électronique utilisateur, et on fait émettre par ledit écran un signal lumineux modulé correspondant audit code personnel ;

- au cours de l'étape (d), on autorise ou non une opération monétaire ;

- le dispositif électronique de sécurisation a en mémoire, au moins un compte d'unités de valeur, et au cours de l'étape (d) on autorise ou non une opération impliquant une modification dudit compte d'unités de valeur ;

- au cours de l'étape (d), des unités sont échangées entre le compte d'unités de valeur du dispositif électronique de sécurisation et un compte d'unités distant géré par un appareil distant relié par des moyens de télécommunication à l'appareil électronique utilisateur ;

- au cours de l'étape (d), après modification du compte d'unités de valeur du dispositif électronique de sécurisation, on fait émettre par l'interface de sortie des informations d'accusé de réception, et on communique ces informations d'accusé de réception à l'appareil électronique utilisateur par l'intermédiaire de l'interface d'entrée dudit appareil électronique utilisateur ;

- au cours de l'étape (a) :

. on fait choisir à l'utilisateur une zone d'écran sur l'écran de l'appareil électronique utilisateur et au cours de l'étape (d) après modification du compte d'unités de valeur du dispositif électronique de sécurisation et

associée à une signalétique visuelle prédéterminée parmi plusieurs zones écrans associées à des signalétiques visuelles différentes, ces zones d'écrans émettant respectivement des signaux lumineux modulés différents porteurs d'informations d'entrée différentes,

. on place le capteur optique du dispositif électronique de sécurisation face à la zone d'écran choisie par l'utilisateur et on capte le signal lumineux modulé émis par cette zone d'écran au moyen dudit capteur optique,

et au cours de l'étape (d), on valide le choix de l'utilisateur en fonction de la vérification du code de sécurisation reçu par l'appareil électronique utilisateur au cours de l'étape (d) après modification du compte d'unités de valeur du dispositif électronique de sécurisation ;

- au cours de l'étape (d), on incrémente un compteur de votes correspondant au choix effectué par l'utilisateur au cours de l'étape (a) si ce choix est validé par la vérification du code de sécurisation ;

- le dispositif électronique de sécurisation a en mémoire des informations indiquant des sessions de vote passées auxquelles a participé l'utilisateur du dispositif électronique de sécurisation, ces informations étant mises par jour au moyen des informations d'entrée au cours de l'étape (a), et au cours des étapes (b) et (c), on inhibe le fonctionnement normal du dispositif électronique de sécurisation si les informations d'entrée reçues pour une nouvelle session de vote indiquent que l'utilisateur a déjà participé à cette session de vote ;

- au cours de l'étape (d), on fait émettre par l'écran un signal lumineux modulé porteur d'un signal d'accusé de réception confirmant la prise en compte du vote de l'utilisateur, et on met à jour les informations de participation dans la mémoire du dispositif électroni-

que de sécurisation uniquement lorsque le capteur optique du dispositif électronique de sécurisation a reçu ce signal d'accusé de réception ;

- les signaux optiques modulés correspondant aux différentes zones d'écran sont modifiés aléatoirement après chaque vote d'un utilisateur ;

- les différentes zones d'écran sont juxtaposées sur l'écran de l'appareil électronique utilisateur ;

- on fait transmettre les informations d'entrée entre au moins deux zones émettrices appartenant à l'écran de l'appareil électronique utilisateur et au moins deux capteurs optiques appartenant au dispositif électronique de sécurisation ;

- on décode des signaux optiques reçus par les deux capteurs optiques en calculant une différence entre lesdits signaux optiques ;

- on détermine un signal binaire en comparant ladite différence avec une valeur seuil, puis on traite ledit signal binaire par filtrage médian ;

- on détermine un signal binaire en comparant ladite différence avec une valeur seuil préalablement déterminée en faisant transmettre un signal de calibration prédéterminé entre les zones émettrices de l'écran et les capteurs optiques ;

- l'une des zones émettrices de l' écran émet un signal optique modulé, tandis que l'autre desdites zones émettrices émet un signal optique constant.

Par ailleurs, l'invention a également pour objet un disque optique pour la mise en œuvre d'un procédé tel que défini ci-dessus, ce disque comprenant une zone de données annulaire entourant une partie centrale dépourvue de données numériques, ce disque optique étant lisible par un appareil électronique utilisateur au moyen d'un lecteur

à faisceau lumineux, lequel appareil électronique utilisateur comprend en outre au moins une interface d'entrée et un écran lumineux, ledit support de données comportant un dispositif électronique de sécurisation qui comprend :

- une interface de réception comprenant au moins un capteur optique disposé dans la partie centrale du disque optique, pour recevoir des informations d'entrée provenant de l'écran de l'appareil électronique utilisateur,
- une interface d'émission adaptée pour émettre des informations de sortie en fonction des informations d'entrée reçues, ces informations de sortie correspondant (directement ou indirectement) à un code de sécurisation destiné à être communiqué à l'interface d'entrée de l'appareil électronique utilisateur,
- et une unité centrale électronique reliée aux interfaces de réception et d'émission et adaptée pour déterminer les informations de sortie en fonction des informations d'entrée et pour faire émettre lesdites informations de sortie par l'interface d'émission ;
- le dispositif de sécurisation comporte en outre un capteur de mouvement.

D'autres caractéristiques et avantages de l'invention apparaîtront au cours de la description suivante de plusieurs de ses formes de réalisation, données à titre d'exemples non limitatifs, en regard des dessins joints.

Sur les dessins :

- la figure 1 est une vue schématique d'un micro-ordinateur pouvant utiliser un disque optique selon une forme de réalisation de l'invention, comprenant un circuit électronique de sécurisation,
- la figure 2 est un schéma bloc du circuit électronique de sécurisation du disque optique de la figure 1, dans une première forme de réalisation de l'invention,

- la figure 3 est une vue similaire à la figure 2, dans une deuxième forme de réalisation de l'invention,

- la figure 4 représente un dispositif électronique de sécurisation selon une autre forme de réalisation de l'invention, en vue de face,

- la figure 5 est une vue en perspective de la face arrière du dispositif électronique de sécurisation de la figure 4,

- la figure 6 est un schéma bloc du dispositif de la figure 4,

- la figure 7 est une vue schématique d'un micro-ordinateur pouvant coopérer avec le dispositif électronique de sécurisation des figures 4 à 6,

- les figures 8 et 9 sont des vues similaires aux figures 1 et 3, dans une variante de l'invention,

- et les figures 10 à 12 sont des vues similaires respectivement aux figures 4 à 6, dans une autre variante de l'invention.

Sur les différentes figures, les mêmes références désignent des éléments identiques ou similaires.

La figure 1 représente un micro-ordinateur 1 comprenant un écran lumineux 1a (écran cathodique, écran à plasma, écran à cristaux liquides rétro-éclairé, etc.), un clavier 1b et un lecteur 2 de disques optiques numériques 3 (CD-ROM, DVD, etc.) ou autres supports de données numériques.

Dans une première forme de réalisation, l'invention a notamment pour but de sécuriser l'utilisation du disque optique 3, en particulier afin d'empêcher les copies illicites de ce disque optique.

A cet effet, le disque optique 3 comporte, en dehors de sa zone de stockage de données 4 et avantageusement dans sa partie centrale 5 dépourvue de données, un

circuit électronique de sécurisation 6.

Ce circuit électronique de sécurisation, qui est représenté sur la figure 2, est intégré dans la matrice de résine du disque optique et comporte :

- une unité centrale électronique 7 (MP) tel qu'un microcontrôleur ou microprocesseur associé à une mémoire 8 (MEM) pouvant être interne audit microcontrôleur ou microprocesseur (on peut utiliser par exemple le microcontrôleur P8WE5032 commercialisé par PHILIPS SEMICONDUCTORS, une division de la société ROYAL PHILIPS ELECTRONICS, Eindhoven, PAYS-BAS, ou encore le microcontrôleur AT89SC commercialisé par la société ATMEL CORPORATION, 2325 Orchard Parkway, San Jose, CA 95131, USA),
- une source d'énergie électrique 9 (BATT.) telle qu'une pile miniaturisée (par exemple, une pile commercialisée sous la marque TMF® par la société BOLDER TECHNOLOGIES CORPORATION, 4403 Table Mountain Drive, Golden, Colorado (CO) 80403, USA), qui alimente le circuit électronique 6,
- au moins un capteur optique 10 (SENS.) tel qu'un phototransistor, une photodiode ou similaire,
- et un transducteur acoustique, de préférence piézo-électrique, tel qu'un haut-parleur ou une sonnerie électronique 11 ("buzzer") commandée par l'unité centrale 7 et émettant par exemple des signaux sonores ayant un spectre de fréquence constant.

Le dispositif qui vient d'être décrit peut mettre en œuvre un procédé de sécurisation qui permet par exemple de vérifier la présence du disque optique 3 original correspondant à une certaine application (programme, base de données, etc.), notamment lors de l'installation initiale de cette application sur le micro-ordinateur 1.

A cet effet, lors de l'exécution par le micro-

ordinateur 1 du programme d'installation de l'application considérée, ce programme génère des informations d'entrée telles qu'un premier code aléatoire, qui est transmis par le micro-ordinateur 1 vers le disque optique 3 par l'intermédiaire de l'écran 1a, sous la forme d'un signal lumineux modulé émis par exemple à partir d'une zone émettrice prédéterminée 17 de l'écran.

A cette occasion, le micro-ordinateur peut :

- commander le lecteur 2 façon à faire sortir le disque optique 3 dudit lecteur,
- et faire afficher sur l'écran un message demandant à l'utilisateur de disposer le disque optique 3 avec son circuit de sécurisation 6 placé face à l'écran et de préférence directement contre ledit écran.

Pour favoriser le bon positionnement du disque optique 3 sur l'écran, le micro-ordinateur 1 peut avantageusement faire afficher sur cet écran un repère 18 qui indique le positionnement du disque optique. Il peut s'agir par exemple d'un cercle lumineux 18 correspondant au diamètre externe du disque optique, d'une ou plusieurs flèches à mettre en correspondance avec des flèches ou similaires apposées sur le disque, ou autre. Le trou central du disque 3 pourrait également être utilisé pour être mis en correspondance avec un repère lumineux affiché à l'écran 1a.

De plus, la face du disque optique 3 qui doit être placée à l'opposé de l'écran 1a, et/ou le cas échéant celle qui doit être placée contre l'écran peuvent avantageusement être repérées par un ou plusieurs marquages prédéterminés apposés sur le disque 3.

Les informations d'entrée peuvent être codées par modulation de l'intensité lumineuse émise par la zone émettrice 17 de l'écran, et/ou par modulation des couleurs

émises par cette zone 17.

Avantageusement, on peut moduler en parallèle à l'intensité lumineuse des trois couleurs élémentaires de chaque pixel de l'écran 1a : on multiplie ainsi par trois le débit de données échangé entre l'écran 1a et le disque optique 3. Dans ce cas, le capteur optique 10 comportera plusieurs éléments sensibles respectivement aux différentes couleurs élémentaires des pixels de l'écran 1a.

Le débit de données pourrait encore être augmenté en faisant émettre les données en parallèle par plusieurs zones émettrices de l'écran 1a, auquel cas le circuit 6 comporterait autant de capteurs optiques 10 que l'on placerait en correspondance avec les diverses zones émettrices.

Compte tenu des fréquences de balayage d'écran habituellement rencontrées, le débit brut des données ainsi émis par l'écran 1a peut éventuellement être supérieur à 25 bits/s et par couleur élémentaire, soit 75 bits/s en utilisant les trois couleurs élémentaires des pixels.

La démodulation du signal lumineux modulé pourra se faire au niveau de l'unité centrale 7, soit par détection de seuils adaptatifs ou non, soit par détection de fronts, de façon connue en soi.

Grâce à cette démodulation, l'unité centrale reconnaît les informations d'entrée qui lui sont communiquées par le capteur optique 10, et détermine des informations de sortie en fonction de ces informations d'entrée : ces informations de sortie peuvent se présenter par exemple sous la forme d'un deuxième code pseudo-aléatoire généré en fonction d'une clé de codage contenue dans la mémoire 8 de l'unité centrale.

Ensuite, l'unité centrale fait émettre les informations de sortie sous la forme d'un signal acoustique par

le transducteur 11.

Ce signal acoustique peut comporter plusieurs trains de signaux sonores (par exemple 3 à 6 trains de signaux sonores) comprenant chacun plusieurs signaux sonores élémentaires rapprochés (séparés l'un de l'autre par exemple par une durée de 0,2 s) et de durée constante. Le nombre de signaux sonores élémentaires de chaque train de signaux sonores est compris entre 1 et un nombre entier prédéterminé n au moins égal à 2 et par exemple égal à 4. Les trains de signaux sonores peuvent être séparés les uns des autres par des périodes de silence au moins égales à une durée prédéterminée (par exemple, ces périodes de silence peuvent être toutes égales à environ 2 s).

Les informations de sortie sont ainsi codées par le nombre de signaux sonores élémentaires de chaque train de signaux sonores.

Le signal acoustique contenant les informations de sortie est écouté par un opérateur humain, lequel opérateur détermine ainsi le deuxième code susmentionné sous la forme d'une suite de chiffres compris chacun entre 1 et n, correspondant respectivement aux nombres de signaux sonores des différents trains de signaux sonores élémentaires successivement émis par le disque 3.

Puis ledit opérateur communique au micro-ordinateur 1 un code de sécurisation fonction dudit deuxième code (en pratique confondu avec ledit deuxième code), par exemple par l'intermédiaire du clavier 1b. Ces opérations sont de préférence guidées par un ou plusieurs messages affichés sur l'écran 1a du micro-ordinateur.

Si le code de sécurisation reçu est bien relié au premier code susmentionné par une relation prédéterminée, le micro-ordinateur 1 autorise alors le déroulement du programme d'installation ; à défaut, il interdit le déroulement normal de ce programme.

Ce contrôle du bon déroulement du programme d'installation peut également être obtenu notamment :

- par un cryptage des données contenues dans le disque optique 3, le décryptage de ces données ne pouvant être réalisé par le micro-ordinateur qu'avec une clé de décryptage qui est fonction du code de sécurisation susmentionné et du premier code susmentionné,

- ou en incluant dans le programme d'installation ou dans un programme contenu dans le disque optique 3 et destiné à être copié dans la mémoire du micro-ordinateur, un branchement vers une adresse de programmation qui ne peut être déterminée qu'en fonction du code de sécurisation susmentionné et du premier code susmentionné.

Les mêmes principes peuvent être utilisés pour contrôler non plus la seule installation, mais l'usage de l'application informatique considérée, en obligeant l'utilisateur à utiliser le disque optique 3 au moins lors du lancement de ladite application.

Dans ce cas, on notera qu'il est possible en outre de contrôler les modalités d'utilisation de cette application informatique en fonction de données incluses dans la mémoire 8 de l'unité centrale du disque optique 3, et de prévoir que l'unité centrale 7 ne renvoie le deuxième code susmentionné que si les conditions d'utilisation requises sont réunies.

A titre d'exemple, on peut ainsi prévoir :

- un nombre maximum d'utilisations ou une durée maximum d'utilisation de l'application informatique,

- ou encore une date à partir de laquelle l'application informatique ne fonctionne plus sauf à racheter un disque optique 3,

- ou encore une limitation des modules de pro-

gramme ou de données accessibles à l'utilisateur (dans ce dernier cas, le processus de sécurisation susmentionné doit être répété à chaque fois que l'utilisateur veut accéder à un nouveau module de programme ou de données).

On notera que le signal acoustique émis par le transducteur 11 pourrait être codé autrement que de la façon décrite ci-dessus, et notamment :

- en faisant émettre ce signal acoustique sous la forme d'une suite de signaux sonores de durées variables séparés les uns des autres par des périodes de silence de durée prédéterminée, les informations de sortie étant codées par la variation de la durée des différents signaux sonores ;

- ou en modulant la fréquence du signal sonore émis (dans ce cas, le spectre de fréquences du transducteur 11 ne doit pas être constant, ce transducteur pouvant prendre la forme d'un haut-parleur piézo-électrique).

En variante, il serait par ailleurs possible de prévoir que le signal acoustique émis par le transducteur 11 soit reçu directement par le micro-ordinateur 1, notamment par l'intermédiaire d'un microphone 12 externe qui est connecté à une carte son interne du micro-ordinateur et qui est approché du lecteur 2 par l'utilisateur au moment opportun, en fonction des indications données sur l'écran 1a du micro-ordinateur.

En pratique, le poste distant 13 peut être constitué notamment par un site internet.

Selon une autre variante, le signal acoustique émis par le transducteur 11 est transmis à un poste de contrôle distant 13 :

- par l'intermédiaire du microphone 12 susmentionné et d'un modem 14 appartenant au micro-ordinateur 1 et relié au poste de contrôle distant 13 par l'intermé-

diaire du réseau téléphonique commuté,

- ou par l'intermédiaire de l'utilisateur téléphonant au poste de contrôle 13.

Dans ce dernier cas, le poste de contrôle distant 13 détermine le code de sécurisation en fonction dudit signal acoustique et transmet ce code de sécurisation au micro-ordinateur 1 par l'intermédiaire du modem 14 (ou bien le code de sécurisation est donné par téléphone à l'utilisateur, qui le tape ensuite sur le clavier 1b du micro-ordinateur). Eventuellement, le poste de contrôle distant 13 peut être amené à ne pas transmettre ce code de sécurisation au micro-ordinateur 1, par exemple si l'utilisation de l'application informatique considérée est soumise à un abonnement qui n'a pas été payé.

Selon une autre variante, représentée sur la figure 3, le transducteur acoustique peut être un haut-parleur 16 associé à un circuit de synthèse vocale 15 lui-même commandé par l'unité centrale 7 : dans ce cas, le haut-parleur 16 émet un message sonore compréhensible par l'utilisateur et contenant les informations de sortie qui correspondent au code de sécurisation. Eventuellement, le circuit de synthèse vocale 15 peut être intégré à l'unité centrale 7, constituée par exemple par un microprocesseur de type TSP50C0x/1x commercialisé par la société TEXAS INSTRUMENTS, Dallas, USA.

On notera par ailleurs que le disque optique 3 pourrait comporter une interface d'émission autre qu'une interface acoustique, par exemple une interface optique.

En particulier, les informations de sortie pourraient également être communiquées à l'utilisateur par l'intermédiaire d'un afficheur 23, en remplacement ou en complément du transducteur 11 ou du haut-parleur 16.

On notera enfin que le processus de sécurisation

autorisé par le disque optique 3 ou autre support de données selon l'invention n'est pas limité au contrôle de l'utilisation de programmes ou de données contenus dans le disque optique : au contraire, ce processus de sécurisation peut être utilisé par exemple pour identifier l'utilisateur, notamment pour permettre des opérations de paiement à distance ou pour permettre un accès à distance à des données protégées, et ce sans qu'il soit nécessaire de doter le micro-ordinateur d'un dispositif de sécurisation spécifique tel qu'un lecteur de cartes à mémoire ou similaire.

Dans ce cas, lorsque le micro-ordinateur 1 est doté d'un microphone 12 et d'un modem 14, le processus de sécurisation débute par l'entrée d'un code secret par l'utilisateur sur le clavier 1b, puis le poste central 13 susmentionné (ou similaire) échange des messages codés avec le circuit de sécurisation 7 du disque optique, pour vérifier la cohérence entre le code entré par l'utilisateur et une clé secrète contenue dans la mémoire 8 de l'unité centrale 7, comme cela est déjà connu pour les cartes de paiement à mémoire.

Un tel paiement à distance pourra être utilisé par exemple pour accéder à de nouvelles fonctionnalités d'un logiciel mémorisé sur le disque optique 3, ou payer une location du logiciel porté par le disque 3. Dans ces deux cas, le poste central 13 (en pratique, un site internet) enverra un code d'accès au micro-ordinateur 1, lequel demandera à l'utilisateur de placer le disque 3 face à l'écran 1a pour pouvoir transférer ce code au circuit de sécurisation 6 du disque par le biais du capteur optique 10. Ce code sera ensuite utilisé par le circuit 6 pour élaborer les informations de sortie en réponse aux informations d'entrée, à chaque nouvel accès de l'utilisateur

auxdites nouvelles fonctionnalités ou au logiciel dans son ensemble.

On pourrait également utiliser un support de données sécurisé tel que décrit ci dessus comme porte-monnaie électronique ou similaire. Dans ce cas, le dispositif électronique de sécurisation 6 peut avoir en mémoire un compte d'unités de valeur (unités monétaires ou similaires), et l'unité centrale 7 dudit dispositif de sécurisation est alors adaptée pour faire varier ledit compte d'unités de valeur en fonction de données codées reçues et émises par l'unité centrale 7 par l'intermédiaire des interfaces de réception et d'émission, par exemple pour recharger le compte lors d'un rachat d'unités de valeur par l'utilisateur ou au contraire pour débiter le compte en fonction d'achats ou d'autres opérations payantes effectuées par l'utilisateur, par exemple sur le réseau internet.

Lorsqu'on utilise le dispositif de sécurisation 6 pour contrôler ou limiter l'usage du support de données, comme déjà indiqué ci-dessus, ou pour établir un profil d'utilisateur, ce dispositif électronique de sécurisation peut également avoir en mémoire un ou plusieurs compteurs d'unités d'utilisation.

Lorsqu'il s'agit de limiter l'usage du support de données, ce compteur peut être représentatif par exemple d'un nombre d'utilisations, et l'unité centrale 7 dudit dispositif de sécurisation peut être adaptée pour incrémenter ou décrémenter ledit compteur en fonction des mises en fonctionnement du support de données, lesquelles peuvent correspondre à des réceptions de signaux optiques modulés par le capteur 10 ou à des détections de rotation du disque 3 par un capteur de mouvement tel qu'un accéléromètre miniature 19 (ACC.) qui pourrait le cas échéant être

intégré au disque 3. Par exemple, l'interface d'émission du dispositif de sécurisation cesse d'émettre les informations codées de sortie qui permettent normalement à l'appareil utilisateur de faire fonctionner le support de données lorsque l'unité centrale 7 a détecté un nombre x prédéterminé de mises en fonctionnement du support de données, c'est-à-dire lorsque le compteur atteint x en partant de 0 ou lorsqu'il atteint 0 en partant de x.

Le capteur 19 pourra par exemple être un micro-capteur (pouvant présenter par exemple une surface de 2 mm sur 2 mm) obtenu par micro-usinage sur silicium, tels que les capteurs 2g et 50g réalisés par le Laboratoire d'Electronique, de Technologie et d'Instrumentation (LETI) du CEA (COMMISSARIAT A L'ENERGIE ATOMIQUE), FRANCE.

Lorsqu'il s'agit d'établir un profil d'utilisateur, le ou les compteurs d'utilisation peuvent par exemple être incrémentés à chaque fois que le disque 3 reçoit un signal optique modulé de l'écran 1a pour accéder à certains modules logiciels, ou lorsque le capteur de mouvement 19 détecte certains mouvements ou certaines suites prédéterminées de mouvements, représentatifs de certaines opérations prédéterminées.

Avantageusement, on peut faire lire le compteur d'unités d'utilisation par un lecteur externe 22 (EXT DRV - figure 2), au moyen d'une interface de communication 21 telle qu'une étiquette électronique (TAG) adaptée pour communiquer avec le lecteur 22 par voie hertzienne et appartenant audit dispositif de sécurisation 6. Une telle lecture du compteur d'utilisation pourra avoir lieu par exemple lors du passage de l'utilisateur dans un magasin commercialisant le support de données. Dans ce cas, le support de données pourra avantageusement être miniaturisé, par exemple au format d'une carte de crédit.

Lorsque le circuit de sécurisation 6 comporte un capteur de mouvement 19, l'unité centrale 7 pourrait le cas échéant être conçue pour bloquer le fonctionnement du circuit 6 lorsque le capteur de mouvement 19 a détecté certains mouvements où certaines séquences de mouvements, par exemple un mouvement de rotation continue pendant une durée supérieure à une limite prédéterminée. Dans ce cas, il pourrait alors être possible de débloquer le fonctionnement du circuit de sécurisation 6 en se connectant à un poste centrale distant 13, par exemple un site internet, et en faisant générer à partir de ce poste central distant un signal codé émis par l'écran 1a de l'ordinateur sous forme d'un signal lumineux modulé qui est reçu par le capteur optique 10.

Dans la forme de réalisation des figures 4 à 7, le circuit électronique de sécurisation 6 n'est pas intégré dans un CD ROM, mais dans un boîtier portatif 30 tel qu'un badge, présentant par exemple sensiblement le format d'une carte de crédit en largeur et en longueur. Ce circuit de sécurisation peut fonctionner comme l'une ou l'autre de formes de réalisation décrites précédemment en regard des figures 1 à 3.

Comme représenté sur les figures 4 et 5, ce boîtier électronique peut comporter par exemple sur sa face avant 31, un écran 32 et un clavier 33, ainsi qu'un haut-parleur 16. On notera que le cas échéant, soit l'écran 32, soit le haut-parleur 16 pourrait être supprimé.

Par ailleurs, la face arrière 34 du boîtier 30 comporte au moins un capteur optique 10 similaire à celui déjà décrit dans les formes de réalisation des figures 1 à 3.

Comme représenté sur la figure 6, le circuit électronique de sécurisation 6 comporte une unité centrale 7

identique ou similaire à celle déjà décrite ci-dessus associée à une mémoire 8, et reliée à l'écran 32, au clavier 33, au capteur 10, à une batterie ou pile 9 et au haut-parleur 16, le cas échéant par l'intermédiaire d'un circuit de synthèse vocal 15.

On notera que l'écran 32 peut être réduit à un afficheur de quelques digits, notamment un afficheur à cristaux liquides, et que le capteur 10 est avantageusement associé à une électronique analogique comprenant notamment un intégrateur permettant de s'affranchir du balayage horizontal de l'écran lorsqu'il s'agit d'un écran cathodique, et un comparateur permettant de s'affranchir des variations de flux lumineux d'un écran à l'autre ou en fonction du réglage de l'écran et/ou de l'éclairement ambiant.

Comme représenté sur la figure 7, le circuit électronique de sécurisation 6 peut être employé comme dans les exemples décrits précédemment de façon à capter un signal optique modulé émis par une zone 17 de l'écran 1a du micro-ordinateur 1, pour recevoir des informations d'entrée provenant dudit micro-ordinateur.

De plus, l'écran du micro-ordinateur peut en outre comporter une pluralité de zones d'écran prédéterminées 35 qui émettent respectivement des signaux optiques différents les uns des autres, correspondant par exemple à différents symboles qui peuvent être affichés en clair dans chaque zone 35 ou à côté de chaque zone 35. Dans l'exemple représenté sur la figure 7, les symboles auxquels sont associés les différentes zones d'écran 35 sont constituées par les dix chiffres allant de 0 à 9.

Les zones d'écran 35 constituent ainsi en quelque sorte un clavier optique permettant à un utilisateur de communiquer des informations à l'unité centrale 7 du circuit électronique de sécurisation, comme il sera expliqué

ci-après.

On notera que lorsque le micro-ordinateur 1 est doté d'un tel clavier optique, le clavier 33 pourrait être fortement simplifié, et pourrait être par exemple réduit à un bouton de validation associé le cas échéant à un bouton de marche/arrêt.

Le fonctionnement du dispositif qui vient d'être décrit est similaire au fonctionnement du dispositif précédemment décrit en regard des figures 1 à 3.

Plus particulièrement, lorsque le micro-ordinateur 1 exécute un programme impliquant par exemple une identification de l'utilisateur, ledit micro-ordinateur peut par exemple demander à l'utilisateur, par un message affiché dans une zone 36 de l'écran 1a, de positionner le capteur optique 10 de son boîtier 30 face à la zone 17 de l'écran 1a, pour recevoir des informations d'entrée.

Pour cela, l'utilisateur active le boîtier 30 au moyen d'un bouton marche/arrêt faisant partie du clavier 33, ou bien cette activation peut être automatique en présentant simplement le capteur optique 10 devant la zone d'écran 17 qui émet un signal optique modulé reconnaissable par l'unité centrale 7 du circuit électronique de sécurisation 6.

Eventuellement, au moins pour accéder à certaines fonctions "sensibles" du boîtier 30, par exemple pour effectuer un paiement en ligne sur internet ou autre, l'utilisateur peut avoir à communiquer un code d'accès à l'unité centrale 7.

Cette communication du code d'accès peut être effectuée de plusieurs façons :

- lorsque le boîtier 30 est pourvu d'un clavier 33 suffisamment complet, le code d'accès peut être tapé par l'utilisateur sur ledit clavier 33,

- le code d'accès peut être tapé par l'utilisateur sur le clavier 1b du micro-ordinateur 1, après quoi le micro-ordinateur 1 émet dans la zone d'écran 17, ou dans une autre zone d'écran prédéterminée, un signal optique modulé porteur dudit code d'accès : l'utilisateur place alors le capteur optique 10 du boîtier 30 face à la zone d'écran 17, de façon que le code d'accès soit transmis à l'unité centrale 7 par l'intermédiaire dudit capteur optique,

- et lorsque l'écran 1a du micro-ordinateur 1 affiche les zones d'écran 35 susmentionnées, l'utilisateur peut positionner successivement le capteur optique 10 face aux différentes zones 35 qui correspondent aux chiffres ou aux autres symboles composant le code d'accès (l'utilisateur valide chaque symbole de son code d'accès en appuyant sur un bouton de validation appartenant au clavier 33 lorsque le capteur optique 10 est situé en face de la zone d'écran 35 correspondant au symbole que veut communiquer l'utilisateur à l'unité centrale 7).

Après activation du circuit électronique de sécurisation 6, l'utilisateur, guidé par les messages affichés dans la zone 36 de l'écran, positionne le capteur optique 10 face à la zone d'écran 17, de sorte que l'unité centrale 7 du circuit électronique de sécurisation reçoit des données d'entrée provenant du micro-ordinateur 1.

La réception de ces données d'entrée peut être déclenchée par appui de l'utilisateur sur un bouton de validation appartenant au clavier 33, comme déjà expliqué précédemment.

De plus, lorsque des données ont été bien reçues par l'unité centrale 7, ladite unité centrale peut faire émettre un signal prédéterminé par le haut-parleur 7 (bien entendu, de tels signaux sonores d'acquit peuvent être

émis également lors de l'utilisation du "clavier optique" constitué par les zones 35 de l'écran 1a, pour entrer un code d'accès ou un autre code dans l'unité centrale 7).

On notera que, lorsqu'on fait communiquer des données au boîtier portatif 30 par un signal optique modulé émis par la zone d'écran 17, la modulation du signal optique peut être réalisée de la façon suivante :

- tout message émis par la zone d'écran 17 débute par un en-tête prédéterminé permettant à l'unité centrale 7 de calibré le signal optique reçu et de se synchroniser avec le signal optique reçu,

- puis les données du message sont transmises sous la forme d'une série de bits émis pendant des fenêtres temporelles successives ayant par exemple une durée de 300 ms, un bit égal à 0 se traduisant par exemple par un signal optique haut (présence d'une émission lumineuse) émis pendant les premières 200 ms de la fenêtre correspondante puis un signal optique bas (absence d'émission lumineuse) pendant les dernières 100 ms de la fenêtre correspondante, tandis qu'un bit égal à 1 se traduit par exemple par un signal optique bas émis pendant les premières 100 ms de la fenêtre correspondante puis un signal optique haut pendant les dernières 200 ms de la fenêtre correspondante

Une fois les données d'entrée reçues par l'unité centrale 7, celle-ci calcule un code de sécurisation qui est fonction desdites données d'entrée et d'autres données.

Ce code de sécurisation peut par exemple être fonction à la fois des données d'entrée reçues par voie optique, d'un code interne mémorisé par l'unité centrale 7, et le cas échéant d'un ou plusieurs paramètres supplémentaires tels que l'heure, la date, un identifiant de

l'utilisateur, un identifiant du micro-ordinateur 1, etc.

Le cas échéant, le code de sécurisation calculé par l'unité centrale 7 peut être également être fonction d'un code personnel de l'utilisateur, que ledit utilisateur doit communiquer à l'unité centrale 7, par exemple par l'un des trois moyens décrits ci-dessus à propos du code d'accès. Dans ce cas, le processus de sécurisation permet non seulement de vérifier la présence du circuit électronique de sécurisation 6, mais également d'identifier ou d'authentifier l'utilisateur, ce qui est extrêmement important notamment pour des opérations de paiement électronique.

A titre d'exemple d'opérations monétaires ou non monétaires réalisables au moyen du dispositif selon l'invention, il est possible notamment de prévoir dans la mémoire 8 de l'unité centrale 7, un compte d'unités de valeur (monétaires ou non) que l'on peut recharger auprès d'une banque ou d'un autre organisme et à partir duquel on peut transférer des unités de valeur vers l'extérieur, notamment pour effectuer des paiements électroniques.

Pour effectuer une recharge d'unités de valeur dans le compte de la mémoire 8, le micro-ordinateur 1 de l'utilisateur peut être mis en connexion, par exemple par internet ou autre, avec le système informatique 13 d'une banque ou d'un autre organisme.

Lorsque cette connexion est établie, l'utilisateur du micro-ordinateur 1 active éventuellement certaines fonctions monétaires de son boîtier 30, comme indiqué ci-dessus, et il s'identifie également comme indiqué ci-dessus, en recevant des informations d'entrée par l'intermédiaire de la zone 17 de l'écran 1a qui sont transmises au boîtier 30 au moyen du capteur optique 10, et en communiquant son code personnel à l'unité centrale 7 également

comme indiqué ci-dessus, après quoi l'unité centrale 7 détermine un code de sécurisation qu'elle communique à l'utilisateur par l'intermédiaire de l'écran 32 et/ou du haut-parleur 16. L'utilisateur tape alors ce code de sécurisation sur le clavier 1b du micro-ordinateur 1, de sorte que ledit micro-ordinateur 1 et/ou le système informatique distant 13 vérifie l'identité de l'utilisateur.

Par ailleurs, le système informatique distant 13 vérifie également que le transfert de crédit demandé par l'utilisateur est possible, par exemple, compte tenu du solde d'un compte 13a de l'utilisateur tenu par le système informatique 13 ou connu de ce système informatique.

Si ce transfert d'unités de valeur est possible, il est alors déclenché par le système informatique distant, de préférence sous forme cryptée.

Le compte d'unités de valeur contenu dans la mémoire 8 de l'unité centrale 7 augmente alors du montant de ce transfert, et de préférence, l'unité centrale 7 fait ensuite émettre un signal d'accusé de réception, sous la forme d'un code qui est affiché sur l'écran 32 et/ou émis par le haut-parleur 16.

Ce dernier code est alors tapé par l'utilisateur sur le clavier 1b du micro-ordinateur 1 pour être communiqué au système informatique distant 13, qui peut ainsi vérifier que le transfert de crédit s'est effectué convenablement.

En variante, le code correspondant au signal d'accusé de réception peut également être transmis vers un tiers de confiance par le micro-ordinateur 1.

Pour transférer des unités de valeur vers une entité externe, c'est-à-dire pour faire une dépense d'unités de valeur, on peut éventuellement utiliser la même procédure que celle indiquée ci-dessus, si ce n'est qu'au lieu

de recevoir des unités de valeur depuis le système informatique distant 13, l'unité centrale 7 reçoit une créance, c'est-à-dire une demande d'unités de valeur qui entraîne une diminution d'autant du compte d'unités de valeur de l'unité centrale 7, et le code d'accusé de réception indique alors l'acceptation du paiement par l'utilisateur du dispositif électronique de sécurisation 6.

Enfin, le dispositif des figures 4 à 7 peut également être utilisé dans une procédure de vote électronique, c'est-à-dire dans une procédure permettant un choix entre plusieurs possibilités et garantissant à la fois l'anonymat du vote et la régularité du vote (en particulier, un utilisateur donné ne doit pouvoir voter qu'une seule fois).

Ce vote pourra par exemple être effectué en faisant afficher des zones d'écran 35, simultanément ou successivement, qui correspondent aux différents choix possibles. de préférence, chacune des zones d'écran 35 est associée à un symbole et/ou à des explications affichées sur l'écran en correspondance avec ladite zone d'écran.

Cette procédure de vote peut par exemple se dérouler comme suit :

- après activation du boîtier portatif 30, l'utilisateur place le capteur optique 10 de son boîtier en face de la zone d'écran 35 correspondant au choix qu'il souhaite effectuer, il valide ce choix au moyen du bouton de validation du clavier 33, et il communique en outre son code personnel à l'unité centrale 7, par l'un des moyens évoqués ci-dessus (si l'entrée du code personnel de l'utilisateur doit être effectuée au moyen d'un "clavier optique", certaines des zones 35 affichées à l'écran correspondront alors à ce clavier optique, tandis que d'autres des zones d'écran 35 correspondent aux différents choix

possibles de l'utilisateur),

- l'unité centrale 7 émet alors un code de sécurisation, au moyen de l'écran 32 et /ou du haut-parleur 16, code qui indique le choix effectué par l'utilisateur sans révéler l'identité dudit utilisateur,

- l'utilisateur tape le code de sécurisation sur le clavier 1b, de sorte que le micro-ordinateur valide le choix de l'utilisateur après avoir vérifié que le code de sécurisation est relié par une relation prédéterminée aux informations d'entrée reçues de la zone d'écran 35 sélectionnée,

- de préférence, le micro-ordinateur 1 fait alors émettre un signal d'accusé de réception par la zone d'écran 17, et affiche un message dans la zone d'écran 36 indiquant que l'utilisateur doit positionner le capteur optique 10 en face de la zone 17,

- l'utilisateur place le capteur optique 10 face à la zone d'écran 17, de sorte que l'unité centrale 7 reçoit le signal d'accusé de réception indiquant que le vote de l'utilisateur a bien été pris en compte,

- le micro-ordinateur 1, et/ou un système informatique distant 13 relié audit micro-ordinateur 1, incrémente un compteur de vote correspondant au choix que vient d'effectuer l'utilisateur,

- et l'unité centrale 7 mémorise des informations indiquant que l'utilisateur vient de participer au vote (le vote auquel vient de participer l'utilisateur peut être identifié par exemple au moyen de certaines informations contenues dans les informations d'entrée initialement reçues par l'unité centrale 7).

Si l'utilisateur souhaite voter une deuxième fois dans la même session de vote, l'unité centrale 7 est avantageusement prévue pour empêcher le déroulement normal du

vote dès lors que l'identification de la session de vote qu'elle reçoit initialement dans les données d'entrée provenant de la zone d'écran 35 sélectionnée correspondent à l'identification d'une session de vote passée qu'elle a en mémoire et à laquelle a déjà participé l'utilisateur du dispositif électronique de sécurisation 6.

De préférence, pour garantir encore plus l'anonymat du vote, en empêchant par exemple qu'un tiers puisse connaître les votes passés de l'utilisateur en s'emparant de son boîtier portatif 30, on peut avantageusement prévoir que l'unité centrale 7 dudit boîtier ne garde aucune trace du choix effectué dans les votes passés. De plus, on peut également prévoir avantageusement que seul le micro-ordinateur 1 puisse déterminer la relation entre les informations d'entrée reçues et provenant de la zone d'écran 35 choisie par l'utilisateur et un vote donné : à cet effet, on peut prévoir par exemple que le micro-ordinateur 1 modifie aléatoirement, notamment après chaque vote d'un utilisateur, les signaux optiques modulés émis respectivement par les différentes zones d'écran 35 qui correspondent aux différents choix offerts à l'utilisateur.

On notera que l'appareil électronique utilisateur pourrait être un terminal de paiement, un terminal de distribution de monnaie réelle ou électronique, un terminal de contrôle d'accès, etc.

Par ailleurs, les figures 8 et 9 représentent une variante de l'invention, similaire aux formes de réalisation des figures 1 et 3, mais qui se différencie de ces formes de réalisation par le fait que le disque optique 3 comporte deux capteurs optiques 10 (SENS1, SENS2) au lieu d'un seul.

De plus, lorsque l'on souhaite transmettre des informations du micro-ordinateur 1 vers le circuit de sécu-

risation 6 du disque optique, on utilise deux zones émettrices 17 de l'écran 1a.

L'utilisateur doit alors placer les deux capteurs optiques 10 de son disque 3 en correspondance respectivement avec les deux zones émettrices 17, de façon que chacun des capteurs 10 reçoive un signal lumineux Sa, Sb provenant de la zone 17 correspondante. Avantageusement, l'écran 1a et le disque optique 3 peuvent comporter des repères permettant la bonne orientation du disque 3 pour que chaque capteur optique 10 soit disposé en face de la zone correspondante 17 de l'écran.

Les signaux Sa, Sb sont générés par les capteurs 10 par exemple sous forme de signaux de courant, auquel cas ils sont de préférence transformés en signaux de tension dans un convertisseur courant-tension avant d'être acheminés vers l'unité centrale 7 du circuit 6. L'unité centrale 7 calcule alors la différence Sa-Sb entre les signaux Sa, Sb (en valeur relative ou en valeur absolue) pour déterminer un signal reçu de l'écran 1a, en s'affranchissant ainsi de l'influence de l'éclairage ambiant.

Avantageusement, l'une des zones émettrices 17, dite première zone émettrice, peut clignoter en transmettant l'information voulue (par exemple, un bit égal à 1 peut se traduire par une période où ladite zone 17 apparaît en blanc tandis qu'un bit égal à 0 peut se traduire par une période où ladite zone 17 apparaît en noir), pendant que l'autre zone 17, dite deuxième zone émettrice, reste inchangée (par exemple noire). La deuxième zone émettrice 17 peut être soit une zone limitée de l'écran 1a, comme représenté sur la figure 8, soit recouvrir la majeure partie de l'écran 1a en dehors de la première zone 17. Les périodes successives au cours desquels la première zone 17 est soit noire, soit blanche, sont de préférences

toutes de même durée ou de durées variables mais répétitives, et la lecture des zones 17 par les capteurs optiques 10 est synchronisée avec ces périodes.

Avantageusement, le signal Sa-Sb est d'abord filtré pour s'affranchir du balayage de l'écran lorsque cet écran est un écran cathodique, puis l'unité centrale 7 compare la différence Sa-Sb ainsi filtrée à une valeur de seuil pour déterminer si elle reçoit un bit égal à 0 ou à 1, après quoi le signal S traité par l'unité centrale 7 est binaire. Cette valeur de seuil peut être prédéfinie, ou être adaptative et déterminée par exemple au cours d'une phase de calibration où le micro-ordinateur 1 fait émettre par les zones 17, un signal connu à l'avance de l'unité centrale 7.

Au cours de cette phase de calibration, réalisée par exemple au début de chaque communication de l'écran 1a vers le circuit de sécurisation 6, on peut notamment faire émettre à la première zone 17 un signal d'en-tête (éventuellement répété plusieurs fois) au cours duquel la première zone 17 émet par exemple un signal haut (couleur blanche) pendant 0,5 s, puis un signal bas (couleur noire) pendant 0,6 s, pendant que la deuxième zone 17 reste noire. La valeur de seuil peut alors être déterminée par exemple en faisant la moyenne de valeurs Sa-Sb mesurées au cours de ces différentes périodes, en sélectionnant le même nombre de valeurs Sa-Sb qui correspondent à signal haut que de valeurs Sa-Sb qui correspondent à un signal bas.

Avantageusement, on peut traiter par filtrage médian le signal binaire S, pour s'affranchir du bruit impulsionnel, très fréquent.

Le signal SM ainsi filtré est obtenu en calculant la valeur médiane du signal S sur 2N+1 échantillons succes-

sifs, constituant une fenêtre glissante de 2N+1 échantillons centrée sur l'échantillon k du signal à calculer : SM(k)=médiane[S(k-N), S(k-N+1), …, S(k), …, S(k+N-1), S(k+N)], ce qui revient à un vote majoritaire des 2N+1 échantillons de S.

La période d'échantillonnage est choisie beaucoup plus courte que la durée des périodes au cours desquelles la première zone 17 conserve une luminosité constante. En choisissant N tel que la durée correspondant à N échantillons successifs soit nettement inférieure à la durée pendant laquelle la première zone 17 est de luminosité constante, on ne perturbe pas la bon décodage des signaux optiques reçus mais on corrige tous les bruits affectant moins de N échantillons.

Eventuellement, les deux zones 17 pourraient émettre toutes les deux des signaux optiques modulés, par exemple en opposition de phase d'une zone 17 par rapport à l'autre. Dans ce cas, c'est le signe de la différence Sa-Sb qui détermine la valeur de chaque bit transmis. On peut appliquer dans ce cas le traitement du signal décrit ci-dessus, mutatis mutandis.

Par ailleurs, comme déjà indiqué ci-dessus pour d'autres modes de réalisation de l'invention, on peut éventuellement multiplier par 3 le débit d'information de l'écran vers le circuit de sécurisation 6 en transmettant des signaux différents respectivement dans les trois couleurs élémentaires utilisées par l'écran si c'est un écran couleur. Dans ce cas, chaque capteur optique 10 comporte trois détecteurs élémentaires correspondant respectivement auxdites trois couleurs élémentaires.

Enfin, comme représenté sur les figures 10 à 12, un boîtier portatif 30 tel que celui des figures 4 à 6 peut également être équipé de deux capteurs optiques 10

destinés à lire deux zones émettrices 17 de l'écran 1a d'un micro-ordinateur 1 ou d'un autre appareil électronique. Le mode de transmission de données depuis l'écran 1a vers les capteurs 10 du boîtier 30, ainsi que le traitement du signal dans le boîtier 30, peuvent être les identiques ou similaires à ce qui vient d'être décrit pour les figures 8 et 9.

REVENDICATIONS

1. Procédé de sécurisation utilisant une transmission d'information par voie optique entre d'une part un appareil électronique utilisateur (1) qui comprend au moins une interface d'entrée (1b, 12) et un écran (1a), et d'autre part, un dispositif électronique de sécurisation (6) qui comprend :

- une interface de réception comprenant au moins un capteur optique (10) pour recevoir des informations d'entrée provenant de l'appareil électronique utilisateur,
- une interface d'émission (11, 16, 23, 32) adaptée pour émettre des informations de sortie en fonction au moins des informations d'entrée reçues, ces informations de sortie correspondant à un code de sécurisation destiné à être communiqué à l'interface d'entrée (1b, 12) de l'appareil électronique utilisateur,
- et une unité centrale électronique (7) reliée aux interfaces de réception et d'émission et adaptée pour déterminer les informations de sortie en fonction au moins des informations d'entrée et pour faire émettre lesdites informations de sortie par l'interface d'émission,

le procédé de sécurisation comprenant les étapes suivantes :

(a) faire transmettre les informations d'entrée par le dispositif électronique utilisateur (1) à l'interface de réception (10) du dispositif de sécurisation,

(b) faire déterminer les informations de sortie par l'unité centrale (7) du dispositif électronique de sécurisation, en fonction des informations d'entrée,

(c) faire émettre par l'interface d'émission (11, 16, 23, 32) du dispositif électronique de sécurisation, les informations de sortie correspondant audit code de sé-

curisation, et communiquer ce code de sécurisation à l'appareil électronique utilisateur, par l'intermédiaire de l'interface d'entrée (1b, 12) dudit appareil électronique utilisateur,

(d) et vérifier que le code de sécurisation reçu par l'appareil électronique utilisateur est relié aux informations d'entrée par une relation prédéterminée,

caractérisé en ce qu'au cours de l'étape (a), on place le capteur optique (10) du dispositif électronique de sécurisation face à l'écran (1a) de l'appareil électronique utilisateur tandis qu'on fait émettre par ledit écran un signal lumineux modulé porteur des informations d'entrée.

2. Procédé selon la revendication 1, dans lequel, au cours de l'étape (d), on autorise ou non certaines opérations réalisées au moyen de l'appareil électronique utilisateur (1), en fonction de la vérification du code de sécurisation.

3. Procédé selon l'une quelconque des revendications 1 et 2, dans lequel le dispositif électronique de sécurisation (6) appartient à un support portatif de données numériques (3) lisible par l'appareil électronique utilisateur (1).

4. Procédé selon la revendication 3, dans lequel le support de données utilisé est un disque optique (3) comprenant une zone de données annulaire (4) entourant une partie centrale (5) dépourvue de données numériques, laquelle partie centrale comprend le capteur optique (10).

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel, au cours de l'étape (a), ledit signal lumineux modulé est émis dans une zone prédéterminée (17) appartenant à l'écran, et on place le capteur optique (10) du support de données au voisinage immédiat de ladite zone prédéterminée.

6. Procédé selon la revendication 5, dans lequel, au cours de l'étape (a), ladite zone prédéterminée (17) de l'écran est signalée par au moins un repère (18) affiché par l'écran (1a).

7. Procédé selon l'une quelconque des revendications précédentes, dans lequel, au cours de l'étape (c), les informations de sortie sont émises par le dispositif électronique de sécurisation (6) sous forme d'un signal acoustique.

8. Procédé selon la revendication 7, dans lequel le signal acoustique contenant les informations de sortie est écouté par un opérateur humain, lequel opérateur détermine le code de sécurisation en fonction du signal écouté et communique ce code de sécurisation à l'appareil électronique utilisateur par l'intermédiaire de son interface d'entrée (1b).

9. Procédé selon la revendication 7, dans lequel le signal acoustique contenant les informations de sortie est reçu directement par l'interface d'entrée (12) de l'appareil électronique utilisateur.

10. Procédé selon l'une quelconque des revendications 7 à 9, dans lequel le signal acoustique contenant les informations de sortie est transmis à un poste de contrôle distant (13) qui détermine le code de sécurisation en fonction dudit signal acoustique et transmet ce code de sécurisation à l'interface d'entrée de l'appareil électronique utilisateur.

11. Procédé selon l'une quelconque des revendications précédentes, dans lequel au cours de l'étape (c), les informations de sortie sont émises par le dispositif électronique de sécurisation (6) par affichage sur un dispositif d'affichage (23, 32).

12. Procédé selon l'une quelconque des revendica-

tions précédentes, dans lequel on fait échanger des données codées entre d'une part, un poste central (13) distant communiquant avec l'appareil électronique utilisateur (1), et d'autre part, l'unité centrale (7) du dispositif électronique de sécurisation, par l'intermédiaire des interfaces d'émission et de réception (11, 16, 23, 32 ; 10) dudit dispositif électronique de sécurisation.

13. Procédé selon l'une quelconque des revendications précédentes, dans lequel le dispositif électronique de sécurisation (6) a en mémoire un compte d'unités de valeur, et l'unité centrale (7) dudit dispositif de sécurisation est adaptée pour faire varier ledit compte d'unités de valeur en fonction de données codées reçues et émises par l'unité centrale par l'intermédiaire des interfaces de réception et d'émission (11, 16, 23, 32 ; 10).

14. Procédé selon l'une quelconque des revendications précédentes, dans lequel le dispositif électronique de sécurisation (6) appartient à un support portatif de données numériques (3) qui est lisible par l'appareil électronique utilisateur (1) avec mise en mouvement dudit support de données, le dispositif électronique de sécurisation (6) ayant en mémoire au moins un compteur d'unités d'utilisation, et l'unité centrale (7) dudit dispositif de sécurisation fait varier ledit compteur en fonction des mouvements du support de données détectés par un capteur de mouvement (10).

15. Procédé selon la revendication 14, dans lequel on fait lire le compteur d'unités d'utilisation par un lecteur externe (22), au moyen d'une interface de communication (21) appartenant audit dispositif de sécurisation (6).

16. Procédé selon l'une quelconque des revendications précédentes, comprenant une étape d'activation d'au

moins certaines fonctions du dispositif électronique de sécurisation (6), étape au cours de laquelle on communique un code d'accès prédéterminé à l'unité centrale (7) dudit dispositif électronique de sécurisation.

17. Procédé selon la revendication 16, dans lequel, au cours de l'étape d'activation, on communique le code d'accès à l'unité centrale (7) au moyen d'une interface d'entrée (33) du dispositif électronique de sécurisation (6) actionnable par un utilisateur.

18. Procédé selon la revendication 16, dans lequel, au cours de l'étape d'activation, on communique le code d'accès à l'unité centrale (7) en positionnant successivement le capteur optique (10) du dispositif électronique de sécurisation (6) en correspondance avec plusieurs zones prédéterminées (35) appartenant à l'écran (1a) de l'appareil électronique utilisateur, ces différentes zones prédéterminées (35) de l'écran (1a) émettant respectivement différents signaux optiques prédéterminés et correspondant chacun à un symbole affiché sur l'écran.

19. Procédé selon la revendication 16, dans lequel, pour communiquer le code d'accès à l'unité centrale (7) du dispositif électronique de sécurisation, on communique d'abord ce code d'accès à l'appareil électronique utilisateur (1) en utilisant l'interface d'entrée (1b) dudit appareil électronique utilisateur, on place le capteur optique (10) du dispositif électronique de sécurisation face à l'écran (1a) de l'appareil électronique utilisateur, et on fait émettre par ledit écran un signal lumineux modulé correspondant audit code d'accès.

20. Procédé selon l'une quelconque des revendications précédentes, dans lequel, au cours de l'étape (b), on fait déterminer les informations de sortie par l'unité centrale (7) du dispositif électronique de sécurisation en

fonction des informations d'entrée et d'un code personnel précédemment communiqué par l'utilisateur du dispositif électronique de sécurisation (6) à ladite unité centrale (7).

21. Procédé selon la revendication 20, dans lequel, au cours de l'étape (b), on communique le code personnel à l'unité centrale (7) du dispositif électronique de sécurisation (6) au moyen d'une interface d'entrée (33) du dispositif électronique de sécurisation (6), actionnable par un utilisateur.

22. Procédé selon la revendication 20, dans lequel, au cours de l'étape (b), on communique le code personnel à l'unité centrale électronique (7) en positionnant successivement le capteur optique (10) du dispositif électronique de sécurisation en correspondance avec plusieurs zones prédéterminées (35) appartenant à l'écran (1a) de l'appareil électronique utilisateur, ces différentes zones prédéterminées (35) de l'écran (1a) émettant respectivement différents signaux optiques prédéterminés et correspondant chacun à un symbole affiché sur l'écran.

23. Procédé selon la revendication 20, dans lequel, au cours de l'étape (b), pour communiquer le code personnel à l'unité centrale (7) du dispositif électronique de sécurisation, on communique d'abord ce code personnel à l'appareil électronique utilisateur en utilisant l'interface d'entrée (1b) dudit appareil électronique utilisateur, on place le capteur optique (10) du dispositif électronique de sécurisation face à l'écran (1a) de l'appareil électronique utilisateur, et on fait émettre par ledit écran un signal lumineux modulé correspondant audit code personnel.

24. Procédé selon l'une quelconque des revendications 20 à 23, dans lequel, au cours de l'étape (d), on

autorise ou non une opération monétaire.

25. Procédé selon l'une quelconque des revendications 20 à 24, dans lequel le dispositif électronique de sécurisation a en mémoire, au moins un compte d'unités de valeur, et au cours de l'étape (d) on autorise ou non une opération impliquant une modification dudit compte d'unités de valeur.

26. Procédé selon la revendication 25, dans lequel, au cours de l'étape (d), des unités sont échangées entre le compte d'unités de valeur du dispositif électronique de sécurisation et un compte d'unités distant (13a) géré par un appareil distant (13) relié par des moyens de télécommunication (14) à l'appareil électronique utilisateur (1).

27. Procédé selon la revendication 26, dans lequel au cours de l'étape (d), après modification du compte d'unités de valeur du dispositif électronique de sécurisation (6), on fait émettre par l'interface de sortie (11, 16) des informations d'accusé de réception, et on communique ces informations d'accusé de réception à l'appareil électronique utilisateur (1) par l'intermédiaire de l'interface d'entrée (1b, 12) dudit appareil électronique utilisateur.

28. Procédé selon l'une quelconque des revendications 20 à 23, dans lequel, au cours de l'étape (a) :

- on fait choisir à l'utilisateur une zone d'écran (35) sur l'écran (1a) de l'appareil électronique utilisateur et au cours de l'étape (d) après modification du compte d'unités de valeur du dispositif électronique de sécurisation (6) et associée à une signalétique visuelle prédéterminée parmi plusieurs zones écrans associées à des signalétiques visuelles différentes, ces zones d'écrans (35) émettant respectivement des signaux lumineux modulés

différents porteurs d'informations d'entrée différentes,

- on place le capteur optique (10) du dispositif électronique de sécurisation face à la zone d'écran (35) choisie par l'utilisateur et on capte le signal lumineux modulé émis par cette zone d'écran au moyen dudit capteur optique,

et au cours de l'étape (d), on valide le choix de l'utilisateur en fonction de la vérification du code de sécurisation reçu par l'appareil électronique utilisateur au cours de l'étape (d) après modification du compte d'unités de valeur du dispositif électronique de sécurisation (6).

29. Procédé selon la revendication 28, dans lequel, au cours de l'étape (d), on incrémente un compteur de votes correspondant au choix effectué par l'utilisateur au cours de l'étape (a) si ce choix est validé par la vérification du code de sécurisation.

30. Procédé selon l'une quelconque des revendications 28 et 29, dans lequel le dispositif électronique de sécurisation (6) a en mémoire des informations indiquant des sessions de vote passées auxquels a participé l'utilisateur du dispositif électronique de sécurisation, ces informations étant mises par jour au moyen des informations d'entrée au cours de l'étape (a), et au cours des étapes (b) et (c), on inhibe le fonctionnement normal du dispositif électronique de sécurisation si les informations d'entrée reçues pour une nouvelle session de vote indiquent que l'utilisateur a déjà participé à cette session de vote.

31. Procédé selon la revendication 30, dans lequel, au cours de l'étape (d), on fait émettre par l'écran un signal lumineux modulé porteur d'un signal d'accusé de réception confirmant la prise en compte du vote de l'utilisateur, et on met à jour les informations de participa-

tion dans la mémoire du dispositif électronique de sécurisation uniquement lorsque le capteur optique (10) du dispositif électronique de sécurisation a reçu ce signal d'accusé de réception.

32. Procédé selon l'une quelconque des revendications 28 à 31, dans lequel les signaux optiques modulés correspondant aux différentes zones d'écran (35) sont modifiés aléatoirement après chaque vote d'un utilisateur.

33. Procédé selon l'une quelconque des revendications 28 à 32, dans lequel les différentes zones d'écran (35) sont juxtaposées sur l'écran (1a) de l'appareil électronique utilisateur.

34. Procédé selon l'une quelconque des revendications précédentes, dans lequel on fait transmettre les informations d'entrée entre au moins deux zones émettrices (17) appartenant à l'écran (1a) de l'appareil électronique utilisateur et au moins deux capteurs optiques (10) appartenant au dispositif électronique de sécurisation (6).

35. Procédé selon la revendication 34, dans lequel on décode des signaux optiques reçus par les deux capteurs optiques (10) en calculant une différence entre lesdits signaux optiques.

36. Procédé selon la revendication 35, dans lequel on détermine un signal binaire en comparant ladite différence avec une valeur seuil, puis on traite ledit signal binaire par filtrage médian.

37. Procédé selon la revendication 35, dans lequel on détermine un signal binaire en comparant ladite différence avec une valeur seuil préalablement déterminée en faisant transmettre un signal de calibration prédéterminé entre les zones émettrices (17) de l'écran (1a) et les capteurs optiques (10).

38. Procédé selon l'une quelconque des revendica-

tions 34 à 37, dans lequel l'une des zones émettrices (17) de l' écran (1a) émet un signal optique modulé, tandis que l'autre desdites zones émettrices (17) émet un signal optique constant.

39.Disque optique (3) pour la mise en œuvre d'un procédé selon l'une quelconque des revendications précédentes, ce disque comprenant une zone de données annulaire (4) entourant une partie centrale (5) dépourvue de données numériques, ce disque optique étant lisible par un appareil électronique utilisateur (1) au moyen d'un lecteur (2) à faisceau lumineux, lequel appareil électronique utilisateur comprend en outre au moins une interface d'entrée (1b, 12) et un écran lumineux (1a), ledit support de données comportant un dispositif électronique de sécurisation qui comprend :

- une interface de réception comprenant au moins un capteur optique (10) disposé dans la partie centrale (5) du disque optique et adapté pour recevoir des informations d'entrée provenant de l'écran (1a) de l'appareil électronique utilisateur,
- une interface d'émission (11, 16, 23, 32) adaptée pour émettre des informations de sortie en fonction des informations d'entrée reçues, ces informations de sortie correspondant à un code de sécurisation destiné à être communiqué à l'interface d'entrée (1b, 12) de l'appareil électronique utilisateur,
- et une unité centrale électronique (7) reliée aux interfaces de réception et d'émission et adaptée pour déterminer les informations de sortie en fonction des informations d'entrée et pour faire émettre lesdites informations de sortie par l'interface d'émission.

40. Disque optique selon la revendication 34, dans lequel le dispositif de sécurisation (6) comporte en outre

un capteur de mouvement (19).

Procédé de sécurisation utilisant une transmission d'information par voie optique et disque optique pour la mise en œuvre de ce procédé.

ABREGE

Dispositif électronique sécurisation comportant une interface de réception (10) optique recevant un signal optique modulé émis par l'écran de l'ordinateur utilisant le support de données, une interface de sortie (11) adaptée pour émettre des informations de sortie en fonction des informations d'entrée reçues, et une unité centrale électronique (7) reliée aux interfaces de réception et d'émission et adaptée pour déterminer les informations de sortie en fonction des informations d'entrée et pour faire émettre lesdites informations de sortie.

FIGURE 2